Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
United States Department of Justice	)	RM No. 11376
	)	
Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act	)	

COMMENTS OF VERISIGN, INC.

Anthony M. Rutkowski
Vice President for Regulatory Affairs and
Standards
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Filed: 25 July 2007

EXECUTIVE SUMMARY

As a leading operator of large-scale critical communications and security infrastructure and provider of CALEA Trusted Third Party services, VeriSign supports the CALEA regulatory model that relies on industry initiative, combined with the Commission arbitrating and overseeing the implementation of necessary requirements for Law Enforcement. In that spirit, the vital capabilities sought in the **Petition for Expedited Rulemaking submitted by the United States Department of Justice (DOJ)** (*Petition*) deserve full, swift, and comprehensive consideration by the Commission. The critically important nature of these needs amply provide the requisite public interest basis for expedited action.

The four capabilities described in the petition can be readily bifurcated in their treatment by the Commission. Time-stamp accuracy and packet activity reporting are well-settled requirements, and extensively available capabilities in most of the communications infrastructure today. There are no significant factual disputes. The Commission can affirm and clarify these requirements by declaration, as well as making a J-STD-025-B deficiency finding. The critical importance of accurate time-stamps deserves an explicit maintenance and traceability requirement such as found in the PacketCable™ CALEA standard – which the Commission can accomplish in a declaration as a compliance clarification and due diligence measure.

The furnishing of reasonably available location information and the secure handover of call-identifying (intercept related) information to law enforcement suggest a need for further fact finding and applying relevant CALEA statutory tests, and is the proper subject of a further rulemaking proceeding. Indeed, the former capability is entwined with the Commission's recently initiated E911 location information proceeding. The implementation of DOJ's desired VPN based handover capabilities is already cost effectively supported today by VeriSign's NetDiscovery Trusted Third Party service. An NPRM will confirm VPN delivery as a highly desirable capability that some industry bodies have already included as part of their CALEA standards.

1. For more than a decade, VeriSign has provided an array of large-scale, ultra-high availability, trusted infrastructures that enable signalling, security, identity management, directory, financial transaction, and fraud management capabilities for just about any kind of network based business and consumer services – whether it be Internet, Web, Internet access, traditional voice telephony, VoIP, multimedia, next generation, or sales. VeriSign operates through various divisions that have offices and staff in the U.S. and worldwide. In these various capacities, it participates in scores of different forums, working collaboratively with both industry and government to find entrepreneurial oriented solutions.

2. As part of these commercial infrastructure support services, VeriSign provides lawfully authorized electronic surveillance (lawful interception) capability requirements to communication providers globally, and participates in or leads many of the related technology, industry, and standards activities.[1] Furthermore, it already provides in conjunction with those services, all the relevant capabilities being sought in the DOJ petition. VeriSign also collaborates closely with industry product vendors worldwide directly and through the Global Lawful Interception Industry Association (GLIIF) whose secretariat it hosts.[2] As a result, VeriSign is a significant interested party uniquely positioned to provide perspective and expert comment concerning the *Petition*.

3. VeriSign also helped pioneer and is today the largest supplier of authenticated time-stamp services. These services for document authentication and commercial transactions are an essential component of trusted commerce and notary services. Authenticated time-stamps – which rely on Trusted Third Parties to provide accurate tamper-proof time-stamps signed with an encrypted digital key – are an example of industry segments going far beyond the rather modest time-stamp capabilities being requested by the DOJ in this proceeding.

---

[1] VeriSign has actively participated in the Lawful Interception related standards Technical Committees of the European Telecommunications Standards Institute (ETSI), CableLabs, OASIS, Alliance for Telecommunications Industry Solutions, and the Telecommunications Industry Association. It is a founding member of the Global LI Industry forum, a Cisco ecosystem partner for implementing its lawful interception products, a contributor to the expert literature in digital forensics, and an active participant at essentially all law enforcement forums and workshops in this sector, including the principal industry tradeshows worldwide, Telestrategies' ISS World.

[2] *See* **Global LI Industry Forum**, http://www.gliif.org

I

THE REQUIRED PUBLIC INTEREST SHOWING OF CRITICAL NEED HAS BEEN MET TO ALLOW THE FCC TO TREAT THE EXPEDITED PETITION

4. The DOJ requests expedited action on the subject petition because the additional and modified capabilities being requested are "critical to terrorism and other criminal investigations and prosecutions will be list, risking both public safety and national security."[3] Furthermore, "if the deficiencies in the standard are not immediately addressed, law enforcement, telecommunications carriers, and equipment manufacturers will be uncertain as to how to proceed, thereby adversely affecting the development and deployment of CALEA solutions for wireless packet data services."[4] As both an infrastructure operator and provider of CALEA Trusted Third Party services, VeriSign concurs on both the criticality and uncertainty bases raised, including the timeliness and the importance of expedited action. Indeed, any delay could perpetuate the potential development and deployment of network elements that fail to support the needed capabilities – thereby exacerbating the national security vulnerabilities.

II

THE PETITION IMPLEMENTS CALEA STATUTORY PROVISIONS AND THE INTENTION OF CONGRESS.

5. At the time of enacting CALEA, Congress made it plain that the communication network environment was highly dynamic, and that continuing collaborative processes would be necessary among the FCC, the FBI and industry.[5] Indeed, many of the dynamic changes in provisioning and technology platforms are recited repeatedly in the Act's legislative history as the basis for its action and specific mechanisms put in place in 1994.

---

[3] *Petition* at n. 4

[4] *Ibid.*

[5] *See* CALEA Legislative History at 3495.

The purpose of H.R. 4922 is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies….

To insure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability….

The legislation leaves it to each carrier to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communication can be intercepted at some point that meets the legislated requirements.

Section 2606 establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations.

Carriers can adopt other solutions for complying with the capability requirements….

The FCC retains control over the standards. Under section 2602(b), any carrier, any law enforcement agency or any other interested party can petition the FCC, which has the authority to reject the standards developed by industry and substitute its own [emphasis added].

[T]he absence of standards will not preclude carriers, manufacturers or support service providers from deploying a technology or service, but they must still comply with the assistance capability requirements.

Subsection (b) provides a forum at the Federal Communications Commission in the event a dispute arises over the technical requirements or standards. Anyone can petition the FCC to establish technical requirements or standards, if none exist, or challenge any such requirements or standards issued by industry associations or bodies under this section.

If an industry technical requirement or standard is set aside or supplanted by the FCC, the FCC is required to consult with the Attorney General and establish a reasonable time and conditions for compliance with and the transition to any new standard. The FCC may also define the assistance obligations of the telecommunications carriers during this transition period.

This section is also intended to add openness and accountability to the process of finding solutions to intercept problems. [6]

---

[6] Summary and Purpose, *id.*

III

TWO OF THE REQUESTED CAPABILITIES – TIME-STAMP ACCURACY AND PACKET SIGNALING INFORMATION - ARE WELL SETTLED MATTERS THAT CAN BE TREATED BY A COMMISSION CLARIFICATION DECLARATION

6. Two of the clarifications requested by DOJ are so well-settled in law as well as deployed technology over many years that the Commission has an ample basis for simply clarifying the requirements regarding time-stamp accuracy and packet signalling information. The only reason the Commission may wish to consider time-stamp accuracy in the context of a rulemaking proceeding in addition to a declaration is to significantly tighten the current 200 millisecond time-stamp accuracy – which is to remedy this rather poor accuracy in light of available contemporary technologies, needs, and industry practice. European authorities have recently proposed a 10 millisecond accuracy requirement to support law enforcement needs.[7]

7. Time-stamps indicate when network events occur. They are the most pervasive network element in communication network and ICT infrastructures. They are essential for almost every operational, administrative, security, and transactional activity. It is not surprising that both time-stamps and the underlying time accuracy support technology were among the first services standardized and deployed in IP-enabled and other packet-mode networks.[8] This early work led to the development of the somewhat revolutionary Network Time Protocol (NTP) as a standard in 1985 and its subsequent deployment throughout packet network infrastructures.[9] NTP has the ability to continuously, automatically measure the setting of an internal computer clock against a national time standard or equivalent, and constantly adjust the computer clock to

---

[7] *See* Agentschap Telecom, *Format for date and time*, ETSI/TC LI Rap#16, Groningen, 27-28 Jun 2007, Doc. ETSI/LI-rap16-td12.

[8] *See, e.g.*, English and Kahn, *Time Standards*, RFCs 28 & 29, Jan 1970; Harrenstien, *Time Server*, Oct 1977; Su, *Specification of the Internet Protocol (IP) timestamp option*, RFC 781, May 1981; Postel and Harrenstien, *Time Protocol*, RFC 868, May 1983;

[9] *See* Mills, *Network Time Protocol (NTP)*, RFC 958, Sep 1985 [superseded by NTP RFCs 1059, 1119, 1305, and 4330].

maintain accuracies in the small millisecond or even microsecond range while also creating an audit trail.

8. Over the past two decades, a global, robust NTP developer community emerged that and resulted in NTP being "baked into" almost every computer operating system and active IP-Enabled network element – including ordinary desktop computers.[10] Almost all NTP software is distributed as free-ware, and set up automatically to run in background with little if any end user intervention. Recent measured deployment of NTP servers using "crawler" technology, confirmed ubiquitous global deployment of NTP servers in the millions with deployed accuracies well under 100 milliseconds.[11] The number of NTP clients is likely in the hundreds of millions. Time-stamps accuracies below one millisecond against the national time standard have become commonplace in network infrastructures, and are essential to everything from maintaining and troubleshooting equipment and forensic analysis of distributed attacks, to resolving disputes among parties contesting a commercially valuable time-sensitive transaction.

9. It is not surprising that law enforcement in 1998-99 sought to implement CALEA time-stamp requirements of 100 milliseconds. Just as accurate time-stamps are critical for the industry, so also are they essential for law enforcement's correlation of distributed communication events, forensic analysis, and potential evidentiary use in criminal proceedings. It is less clear why the requirements were opposed by some parties, but the result was the adoption by the Commission within its own Rules of an explicit 200 millisecond time-stamp accuracy requirement in 1999, and its subsequent application to IP-enabled services in 2006.[12]

10. Some CALEA industry standards body activities – notably CableLabs PacketCable 2.0 and (derivatively) the Cisco Service Independent Intercept (SII)

---

[10] *See, e.g.,* NTP Public Services Project, < www.ntp.org>.

[11] *See* Murta, Torres, and Mohapara, *Characterizing Quality of Time and Topology in a Time Synchronization Network*, IEEE Globecom, Dec 2006.

[12] *See In the Matter of Communications Assistance for Law Enforcement Act in CC Docket No. 97-213, Third Report and Order*, 14 FCC Rcd 16794, 16835 ¶95 (1999) ("*Third R&O*"), *aff'd in part and vacated in part by United States Telecom. Ass'n v. F.C.C.*, 227 F.3d 450,465 (D.C. Cir. 2000); *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services in ET Docket No. 04-295, Second Report and Order and Memorandum Opinion and Order*, May 12, 2006, FCC 06-56.

Architecture specifications – have been supportive in implementing the Commission's time-stamp accuracy standard.[13] (See Appendix A – CALEA Time-Stamp Accuracy Standards). CableLabs in particular produced a comprehensive time-stamp accuracy section in its CALEA standard that effectively implements the Commission's 200 millisecond accuracy rule, including mandated use of NTP. The action recently won recognition by the Assistant Director of the FBI's Quantico Engineering Research Facility.

11. Notwithstanding the rather explicit CALEA time-stamp accuracy standard in the Commission's rules, other industry CALEA standards activity has witnessed consistent efforts over the past several years to effectively eliminate the requirement. Three avenues were pursued: suggesting that the requirement somehow does not apply to packet-mode communications, or that it can be redefined as an internal network time-delay requirement, or that the term "accuracy" can be construed to reference any local time source rather than the national time standard. See Appendix A. These results have led to the deficiency challenge in the DOJ petition.

12. The most expeditious treatment of the petition with respect to time-stamp accuracy is to simply declare that the 200 millisecond accuracy requirements of Sec. 1.0007(a)(14) of the Commission's Rules apply to all CALEA carriers and that minimal due diligence proof of performance requirements apply to assure traceability to the U.S. national standard, such as found in the PacketCable™ CALEA standard. The critical importance of accurate time-stamps deserves an explicit maintenance and traceability requirement. In addition, notice and comment should be sought in a Notice of Proposed Rulemaking that leads to a much better accuracy value, e.g., 10 milliseconds, appropriate to the needs and capabilities extant today. See Appendix B.

13. Packet-activity is a term used to describe an obligation under CALEA for an Internet access provider to provide a capability to isolate and hand over to law enforcement the network signaling information of a suspect pursuant to a court order. This signaling information typically includes – to the extent reasonably available -

---

[13] *See* CableLabs, *PacketCable Electronic Surveillance, Delivery Function to Collection Function Interface*, Specification, PKT-SP-ES-DCI-I01-060914, September 14, 2006.

- the identity of the intercept access point
- the exact time the communication was observed at that point
- identities of the service, session, and subscriber (or subscriber device)
- IP addresses of the intercept subject, source of the communication, and destination
- authentication header security parameters and data
- virtual private network (VPN) tunnel related information, when used
- transport layer protocol
- source and destination ports
- type of IP service

Except for the VPN related information, the international lawful interception used in most countries outside the U.S. includes significantly more information.

14. This signaling information is minimally essential for any forensic analysis, including that undertaken by law enforcement, to understand almost anything about the kind of communication taking place at the access point to an IP network. It is the modern-day equivalent of what was known as "pen register" and "trap and trace" in the legacy telephone access network world. This information is found in the IP packet headers that are analyzed by service providers as part of the ordinary process of providing access service to customers, as well as managing and protecting their access infrastructure. It can usually be extracted for specific subscriber communications within the equipment supporting the access service – usually with the simple addition of available software to that equipment to support CALEA or its equivalent in other countries. This information is used for signaling and network routing within the network and not normally seen (or even known about) by the end user customer.

15. The ability to extract some of this information, especially port numbers, was left out of an industry standard being offered as CALEA compliant, and is challenged by the U.S Department of Justice as deficient - pursuant to the CALEA statute. Some parties argue that port numbers constitute content rather than signaling because there may be an indirect nexus between port numbers and the kind of application being supported. For example, a packet indicating the use of port 80 would indicate use of the World Wide Web. However, no content is provided in handing over this signalling formation and it is difficult to understand how port numbers could realistically be construed as anything

other than call data information. The Commission should declare port numbers and similar packet signaling information to be call data information.

IV

THE REMAINING TWO CAPABILITIES - REASONABLE LOCATION INFORMATION HANDOVER AND SECURE VPNs - ARE APPROPRIATE FOR A NPRM

16. The furnishing of reasonably available location information and the secure handover of call-identifying (intercept related) information to law enforcement suggest a need for further fact finding and applying relevant CALEA statutory tests, and is the proper subject of a further rulemaking proceeding. Indeed, the former capability is entwined with the Commission's recently initiated E911 location information proceeding.

17. The implementation of DOJ's desired VPN based handover capability is a critical need that has become an essential CALEA mechanism. In an IP-enabled network world where law enforcement may need to quickly implement distributed intercept capabilities, including among multiple providers, to obtain necessary target intercept signaling information or content, the use of VPNs are essential. Where there significant broadband data streams involved, some kind of secure buffering may be needed, but the baseline capability should be sufficient in-place VPN capacities and overheads to accommodate the needs. The principal global lawful interception industry standards body recognized these needs several years ago and developed specifications for this capability that now exists as the norm used worldwide.[14] The principal cable industry handover specification has similar functionality.[15] CALEA Trusted Third Party providers like VeriSign offer VPN capabilities automatically as part of the support service with the necessary high bandwidth VPN implementations in place between carrier customers and secure mediation facilities as well as between those facilities and major law enforcement monitoring facilities.

---

[14] *See* European Telecommunications Standards Institute (ETSI), *Technical Specification Lawful Interception (LI), Handover Interface and Service-Specific Details (SSD) for IP delivery, Part 1: Handover specification for IP delivery*, Doc. ETSI TS 102 232-1 V2.1.1 (2006-12).

[15] *See* CableLabs, *PacketCable Electronic Surveillance, Delivery Function to Collection Function Interface*, *supra* n. 13.

Appendix A
Table of Time-Stamp Accuracy Provisions Found in Current CALEA/LI Standards

Time-Stamp Standard	Text	Notes
FCC Rule: 47 CFR §1.20007(a)(14)	A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function...with the call event time-stamped to an accuracy of at least 200 milliseconds.	This is the FCC-adopted CALEA standard applicable to all carriers under CALEA
PacketCable™ 2.0 PKT-SP-ES-DCI-I01-060914	A.4 Timing Information The PacketCable Electronic Surveillance Specification relies on multiple components (CSCFs, MGC, MG, DF) to gather and deliver call data and Call Content to the LEA. Once the call data and Call Content are delivered to the LEA, the LEA will rely on timestamps in the various messages to correlate the reported events. In order to ensure the LEA has sufficiently accurate timing information, PacketCable network elements that generate Event Messages (CSCFs, CMTS, MGC) or timestamp RTP packets (DF) MUST use Network Time Protocol (NTP) time synchronization as defined in [RFC 1305]. 8 CALL DATA CONNECTION (CDC) INTERFACE The PCESP messages MUST contain a timestamp that identifies the time the corresponding event was detected by the IAP. This timestamp MUST have an accuracy of at least 200 milliseconds.	This standard meets both the FCC rule and adds complete mandatory NTP based accuracy capabilities.
TIA/EIA/IS-J-STD-025-A	4.7 Timing Information This capability permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function ...with the call event timestamped to an accuracy of at least 200 milliseconds. This capability places timing requirements on call-identifying message generation after triggering events that shall be met for these messages. It also requires time stamp accuracy for call events	This standard restates the FCC rule
TIA/EIA/IS-J-STD-025-B	[Same as 025-A, except the FCC rule is not expressly included for cdma2000 packet data (Sec. 4.9.2), references ETSI TS 33.106, 33.107, and 33.108 specifications for GPRS/UMTS (Sec. 4.9.3), and ATIS-PP-100678.2006 for VOP in wireline telecommunication networks (Sec. 4.9.4)]	This standard seems to omit the FCC rule for non circuit-mode networks – both expressly and by referencing other standards that omit the FCC rule.
ATIS-PP-100678.2006 [VoIP]	5.4.2 Timing Information Timing information enables law enforcement to associate CII with the content of communication. Timing information includes two elements: a) Event Time-stamp: Each surveillance message shall contain a time-stamp that is recorded within a specific amount of time from when the event triggering the surveillance message was detected (i.e., the time difference between the time the CmII triggering event was detected and the time recorded in the time-stamp). … The following timing requirements shall apply to the delivery of CmII: ... – Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CmII event triggering the surveillance message was detected. The time-stamp shall include a Greenwich Mean Time (GMT) offset, if available	This standard omits the FCC rule - restating it as a delay requirement with archaic (not-recommended) time-stamp term *GMT*.
ATIS-1000013.2007 [Internet Access]	5.3.2 Communications Delivery ... Timing information includes two elements: a) Event Time-stamp: Each surveillance message shall contain a time-stamp that is recorded within a specific amount of time from when the event triggering the surveillance message was detected (i.e., the time difference between the time the CmII triggering event was detected and the time recorded in the time-stamp). … The following timing requirements shall apply to the delivery of CmII: ... – Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CmII event triggering the surveillance message was detected. The time-stamp shall include a Greenwich Mean Time (GMT) offset, if available	This standard omits the FCC rule - restating it as a delay requirement with archaic (not-recommended) time-stamp term *GMT*.

ATIS-0700005-2007 [IMS VoIP & Multimedia]	4.4.2 Timing Requirements Timing information enables LEA(s) to associate CII with the content of communication. Timing information includes two elements: 1) Event Time-stamp - Each event report shall contain a time-stamp that is recorded within a specific amount of time from when the event triggering the surveillance message was detected (i.e., the time difference between the time the CII triggering event was detected and the time recorded in the time-stamp). … • A CII message shall be sent from the TSP's IAP to the LEA's CF within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the CII event time-stamped to an accuracy of at least 200 milliseconds as defined in [99-230]. • If the GMT offset, as defined in [X-680], of the CII IAP is available at the CII IAP or available at the MF/DF, it shall be reported as part of the timestamp information.	
Cisco RFC3924 + V2TapMIBs	[Inherits SNMPv3 values which imports related time-stamp capabilities, including Cisco OS NTP values that should be will within the FCC rule.]	This standard implicitly supports the FCC rule, but may be dependant on the implementing mediation and handover standards.
ETSI/3GPP TS 133 108 V6.10.0 (2005-12) [UMTS]	6.2.1 Timing As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible. NOTE: If the transmission of IRI fails, it may be buffered or lost. Subject to national requirements, the following timing requirements shall be supported: … - Each IRI data record shall contain a time-stamp, based on the intercepting nodes clock, that is generated following the detection of the IRI triggering event. **TimeStamp** FROM HI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1) version7(7)}; -- from ETSI HI2Operations TS 101 671v2.11.1	This standard omits the FCC rule and inherits 1 second accuracy requirement of TS 101671

ETSI TS 101 671 V2.15.1 (2006-11) [generic switched-circuit and packet data]	**TimeStamp** ::= CHOICE
	{
	-- The minimum resolution required is one second.
	-- "Resolution" is the smallest incremental change that can be measured for time and
	-- is expressed with a definite number of decimal digits or bits.
	localTime [0] LocalTimeStamp,
	utcTime [1] UTCTime
	}
		This standard omits the FCC rule and specifies 1 second resolution accuracy.

ETSI TS 102 232 V1.5.1 (2006-10) [IP handovers]	B.8 Other R37) All IRI shall contain a timestamp (TS 101 671 [4], clause 8).	This standard omits the FCC rule and inherits 1 second accuracy requirement of TS 101671.
ETSI TS 101 909-20-1 V1.1.2 (2005-10) [Cable VoIP]	8.4.2.1.3 Timestamp Each IRI Record shall contain a timestamp indicating when the interception was made. The header of TARGETACTIVITYMONITOR information flow shall contain a mandatory timestamp information element. This element shall be of the type defined below: *UTCTime*	This standard omits the FCC rule and inherits 1 second accuracy.
ETSI TS 101 909-20-2 V1.2.1 (2006-03) [Streamed multimedia]	6.4.2.1.3 Timestamp Each IRI Record shall contain a timestamp indicating when the interception was made. The header of TARGETACTIVITYMONITOR information flow shall contain a mandatory timestamp information element. This element shall be of the type defined below: *UTCTime*	This standard omits the FCC rule and inherits 1 second accuracy.

Time-Stamps and CALEA

Frequently Asked Questions

1. What are time-stamps?

   Time-stamps are simply an expression of the time associated with some event. A commonplace example is found on employee time cards that describe the time at which a person began or ended a workday.

2. What are time-stamps used for?

   Time-stamps have been used since the origins of society as part of the records of human events. In modern electronic communication networks, they are used extensively for network operations, administration and management.

3. How are time-stamps used for CALEA?

   CALEA requires a capability of reporting to law enforcement when communications or other network activity of a suspect occur. This is done by sending messages to law enforcement officials including time-stamps – which are an essential common CALEA capability. Thus a CALEA message to law enforcement might read: suspect 12345 called the telephone number 1-888-225-5323 at [2007 06 17 at 14.05.050 hours]. The part in brackets is the time-stamp. Time-stamps are already used for circuit-switched network CALEA compliance.

4. Are time-stamps more important for IP-networks?

   Time-stamps for packet-switched IP-networks are essential and more important than for circuit-switched platforms because signalling events occur asynchronously across large numbers of autonomous, distributed networks. In other words, there is no centralized timing and control as there is in circuit-switched networks. Thus, absent the binding of accurate time-stamps to communication events, the resultant information is effectively worthless for meaningful forensic analysis. This need for accurate time-stamps for management and protection of IP-enabled infrastructure led very early to the development and widespread deployment of technology that provides very accurate time-stamps. Indeed, the lawful interception standards developed by Cisco leverage the same network management time-stamp accuracy capabilities. Similarly, the careful attention to time-stamp accuracy in the CableLabs specifications also benefit cable network operations and administration.

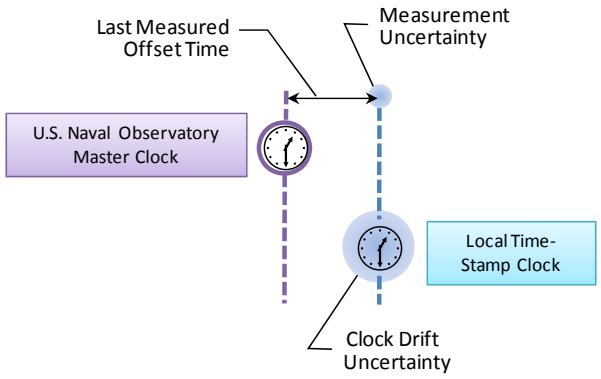
5. Why are accurate IP-network time-stamps important for law enforcement and national security?

   Accurate IP-network time-stamps are important for law enforcement and national security for the same reasons that they are important for network management and protection – the integration and analysis of frequently highly distributed time-stamped event information. Furthermore, the derivative pattern and correlation analysis enabled by accurate time-stamps are often essential in identifying a suspect and understanding the sequence of events. Correlation with content

derived from disparate remote sites in an IP-network environment – especially for VoIP – is highly dependent on accurate time-stamps. Where the information subsequently is introduced in a criminal proceeding, time-stamp accuracy may be highly relevant to the integrity of the evidence in a judicial proceeding.

6. What is time-stamp accuracy?

   Time-stamps are generated by clocks. In the world of time technology, accuracy refers to the known time difference (offset) of the time-stamp clock from the national time reference - the U.S. Naval Observatory Master Clock. For the time offset to be known, however, it must be periodically measured. Between those measurements, the clock offset will drift within a known range of uncertainty. In addition, all time measurements themselves have known uncertainty. As a result, the accuracy of a time-stamp clock at any point in time is determined by a combination of last known offset combined with the clock and measurement uncertainties. See figure below.



   In this figure, if the last measured offset from the U.S.N.O. Master Clock was minus 5 milliseconds, and the measurement uncertainty was 3 milliseconds, and the clock's uncertainty between measurement intervals was 10 milliseconds, the time-stamp can be said to have an accuracy of 18 milliseconds.

7. How are time-stamps made accurate?

   Time-stamp accuracy is determined by the accuracy of the time-stamp clock. Thus accuracy is achieved by using a clock that can be maintained and shown to be within a specified accuracy. Fortunately, widely available software such as Network Time Protocol (NTP) clients exist for doing this automatically to achieve very good accuracies on the order of a few milliseconds or better.

8. What is time traceability?

   Time traceability is the ability to measure the time of a local clock against the national time reference clock – the U.S. Naval Observatory Master Clock. Federal Weights and Measures statutory requirements designate the National Institute of Standards and Technology (NIST) as the responsible agency for all national physical standards. In the case of time, this responsibility is shared with the U.S. Naval Observatory (U.S.N.O.) which is responsible for the nation's Master Clock. U.S.N.O. facilitates this process by providing redundant, very high availability NTP servers such as tick.usno.navy.mil and tock.usno.navy.mil which currently

handle loads of 10 thousand NTP queries per second. Numerous alternative publicly-available slave clocks of equivalent stratum-1 accuracy exist in major IP backbone networks.

9. What is an authenticated time-stamp?

   An authenticated time-stamp is a notary service that securely supports non-reputable assertions of proof that a datum occurred at a particular time. The service is provided by a Time Stamping Authority (TSA) which signs the time-stamp with the TSA's digital key pursuant to well-know standards such as RFC3161. Authenticated time-stamps are used where additional trust in the accuracy of time-stamps is required by law or security or commercial practice. Most major providers of digital certificates provide TSA services. Law enforcement typically has not required authenticated time-stamps, although this could change if judicial systems enforce more strict evidentiary requirements for digital forensics.

10. What is the history of CALEA and time-stamps?

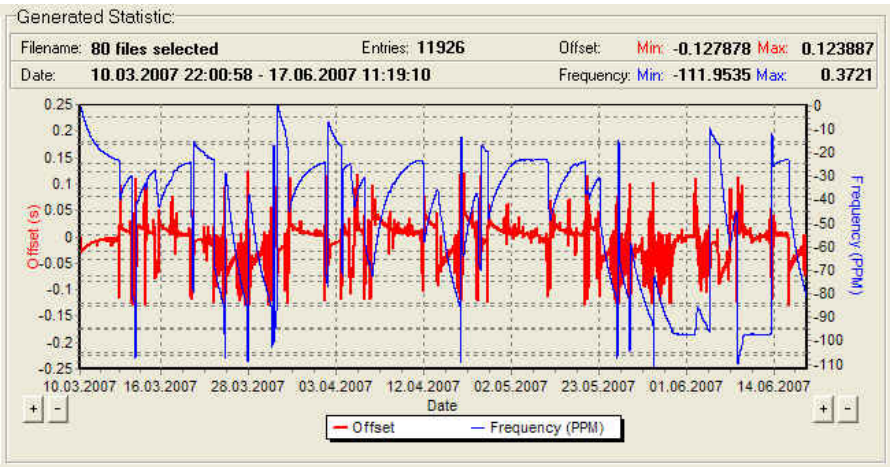
    The Communications Assistance for Law Enforcement Act of 1994 (CALEA statute) requires telecommunication and IP-Enabled services providers to have the ability to isolate and hand over to law enforcement pursuant to a court order the call-identifying information such as signalling that is associated with a suspect's communications. Every signalling event necessarily has an associated time-stamp. In the years following its enactment, the CALEA standards process failed to produce agreement on the accuracy specification. FBI sought a 100 millisecond time-stamp accuracy. The Telecommunications Industry Association offered 200 milliseconds, and the FCC adopted that value as a standard in their own Rules in 1999, and affirmed application to IP-Enabled networks in 2006. Over the past several years, however, some industry standards bodies have sought to redefine the requirement or argued that it somehow doesn't apply to packet networks, although notice was repeatedly provided in standards body contributions that this would make the standards deficient.

11. Why are some CALEA time-stamp specifications deficient?

    Some industry standards bodies like CableLabs have brought together industry experts and produced time-stamp specifications that fully comport with the FCC and FBI requirements as well as good practice. However, other standards bodies such as TIA and ATIS have adopted specifications that either a) implicitly use a one second accuracy value which is inadequate to meet the operational needs of lawful surveillance in IP packet networks, or 2) effectively eliminate accuracy altogether through technical redefinition of the FCC time-stamp accuracy rule. In addition there is no provision made for important time-stamp accuracy maintenance and traceability capabilities such as those widely adopted in the IP networking industry and included in the CALEA standards adopted by CableLabs.

12. How does NTP assure time-stamp accuracy maintenance and traceability?

The time-stamp accuracy maintenance and traceability platform adopted by CableLabs and most of the IP network industry is the widely deployed Network Time Protocol. NTP software continually compares the national master time reference clock to the internal clock that generates the time-stamp in a network device. The drift of the internal clock is automatically measured and adjusted to be very accurately aligned with the master time reference clock. The accuracy and uncertainty of this process is also monitored by the NTP software and can be checked at any time. The figure below shows in the red trace, how the ordinary desktop computer used to prepare this FAQ has operated within an accuracy of 128 milliseconds worst case of the U.S. Naval Observatory Master Clock over a two month period.



Normally the same clock maintains an accuracy of only a few milliseconds, as can be checked at any time by a simple NTP query command as shown in the figure below. In the example, the desktop clock of the desktop computer used to prepare this FAQ is shown to be within 390 microseconds of the USNO master clock with an uncertainty of 5 milliseconds.

```
C:\Users\trutkowski>ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*tick.usno.navy. .USNO.           1 u   17  128  377   17.449   -0.390   4.889
+navobs1.oar.net .USNO.           1 u   92  128  377   16.437   -1.405   3.944
```

13. How do you get NTP software?

NTP software has been bundled with essentially all IP-network equipment operating software for many years and is automatically started at the time the equipment is turned on. This practice was extended to common consumer computer systems about five years ago. The software is also widely available as freeware, and has a large and active developer community that is devoted to perfecting and expanding the use of the platform. See www.ntp.org The underlying protocol standard was first adopted as RFC958 in 1985, and the current version is RFC1305. A very simple new version known as SNTP has recently adopted in the form of RFC4330 for low accuracies in the range of "fractions of a second." The NTP freeware packages typically install automatically in seconds with little required knowledge or intervention.

14. How widely deployed is NTP in IP-enabled networks and what accuracies are maintained?

    Over the past twenty years since the creation of the NTP technology platform, its value proposition has resulted in very widespread deployment. The NTP developer community has periodically instituted automated survey "crawls" across the entire public IP infrastructure determining the number of NTP servers and what accuracies are maintained. The number of NTP clients deployed is not possible to determine; however considering it is bundled with all significant computer operating systems, it is essentially ubiquitous. In 1999, a MIT survey found 647 thousand NTP servers. Testing 175 thousand of them, it was found that 97% had a mean accuracy of better than 20 milliseconds (i.e., 10 times better accuracy than required by the FCC). By 2005, a Stanford survey showed that the number had doubled and accuracy had significantly improved. NTP community demonstrations of different combinations of NTP software, operating systems, and machines indicate consistent accuracies on the order of a few milliseconds. See <www.david-taylor.myby.co.uk/mrtg/daily_ntp.html>

15. Are other low-cost time-stamp accuracy platforms available?

    Global Positioning System (GPS) service relies upon highly stable satellite based clocks that provide time accuracies on the order of 10 nanoseconds (20 million times better than presently required by the FCC for CALEA).. The increasing deployment of low-cost GPS chip sets in network devices provides the ability to implement widespread time-stamp accuracies of a few microseconds – 100 thousand times better than the FCC's current CALEA requirement.

16. Is maintaining required CALEA time-stamp accuracies costly?

    Even the most simple computer today, when it is turned on, ordinarily uses NTP and keeps its internal clock for its own time-stamping at accuracies under 100 milliseconds. A provider seeking to be CALEA compliant, need only verify that its time-stamp clocks are running NTP to maintain the 200 millisecond requirement – a very minimal and low-cost task. If the software for some reason is not there or not functioning, a basic craft level technician or security staff or a CALEA trusted third party representative can correct the problem. Good practice also dictates occasional verification that required accuracy is being maintained as described above – something the FCC in the frequency assignment arena calls proof-of-performance.

17. Is maintaining required CALEA time-stamp accuracies subject to implementation delays?

    As noted above, NTP deployment on network devices is already ubiquitous, and simple, low-cost checks are all that's needed.

18. Are special standards actions or processes necessary to provide required time-stamp accuracies?

    No. The required provision is already found today in § 1.20007(a)(14) of the Commission's Rules. The CableLabs additionally required a mandatory NTP-based proof-of-performance for all cable operators in the specification. The time-

stamp provisions are freely, openly available at PKT-SP-ES-DCI-I01-060914 which has recently received kudos from the FBI's Quantico Laboratory.

19. Does CALEA time-stamp accuracy requirements have anything to do with individual IP packet time-stamps?

    Although time-stamps are also used in asynchronous packet networks to sequence received packets in the proper order, the subject has nothing to do with CALEA. The transfer of individual communication packets among routers in a provider's network is not within the scope of CALEA, and there is no requirement to extract individual packet time-stamps.

20. What kind of actions could the FCC take in response to the recent DOJ petition on time-stamp deficiencies in some industry standards?

    The FCC could simply respond to the petition by declaring that the existing FCC time-stamp accuracy rule of 200 milliseconds exists, and standards bodies should not be seeking to impede its application, but instead facilitate it as did CableLabs for the cable television industry. It would be useful, however, for the FCC to include the subject in a new rulemaking proceeding that would reveal that 200 milliseconds is woefully inadequate today and impose an accuracy requirement similar to the 10 milliseconds proposed by Dutch regulatory authorities, together with a proof-of-performance requirement. See, generally, FCC Docket RM-11376 Petition for Rulemaking.

21. Where can I find out more?

    An extensive White Paper providing substantial background information on Accurate Time Keeping for Lawful Access and Interception is available from the Global LI Industry Forum website.